🛠️ Ejercicio Práctico

📌 **Título:** Evaluación y Mejora Continua de la Seguridad en una API RESTful

---

🎯 Objetivo:

Evaluar un entorno de seguridad para una API RESTful expuesta públicamente, identificar brechas operativas, y proponer un plan de mejora utilizando **métricas, monitoreo continuo, pruebas de penetración y controles de acceso**.

🧱 Escenario:

La empresa **SecureConnect** cuenta con una API RESTful para gestionar la autenticación y consulta de clientes. Durante una revisión de rutina, se detectan las siguientes situaciones:

1. El sistema no registra ni analiza los logs de acceso ni de errores.
2. No existen KPIs definidos para evaluar el rendimiento de las medidas de mitigación.
3. No se realizan pruebas de penetración periódicas en la API.
4. Las respuestas de error muestran detalles sensibles como cabeceras internas y rutas.
5. Los errores 403 y 500 ocurren con frecuencia, pero no están documentados ni correlacionados.

📋 Actividades:

1. **Identifica y explica al menos 4 debilidades de seguridad en el escenario presentado.**
2. **Propón una medida de mejora o control específico para cada debilidad.**

3. **Sugiere al menos 2 KPI útiles para esta API RESTful que ayuden a medir el estado de su seguridad.**

4. **Describe brevemente cómo implementar un sistema de monitoreo continuo usando herramientas open source o comerciales.**

📌 Formato sugerido para la tabla:

Debilidad Identificada	Medida Correctiva o Control Propuesto	Justificación Técnica
Falta de logs de acceso y errores		
Ausencia de métricas de seguridad (KPI)		
No realizar pentesting en la API		
Respuestas de error con detalles internos		

📋 KPI sugeridos (para actividad 3):

- % de reducción mensual de errores 5XX
- Tiempo promedio de resolución de alertas (MTTR)
- Tasa de autenticaciones fallidas por hora
- Número de endpoints escaneados con resultado crítico

💡 Recomendaciones:

- Considera herramientas como:
    - **ELK Stack (Elasticsearch, Logstash, Kibana)**
    - **Wazuh o Splunk para SIEM**
    - **OWASP ZAP o Burp Suite para pruebas de seguridad**

- **Grafana + Prometheus para visualización de métricas**

📦 Entregables esperados:

- Tabla con al menos 4 riesgos reales y sus respectivas propuestas.
- Descripción de 2 KPI con su propósito y forma de medición.
- Explicación clara y aplicable del sistema de monitoreo sugerido.
